REMARKS

The Examiner is thanked for the thorough examination of the present application, the agreement that all claims define over the previously applied references, and the corresponding withdrawal of all prior rejections. The Office Action, however, has continued to reject all claims 1-16. Specifically, claims 1-16 are now rejected under 35 U.S.C 102(e) as allegedly anticipated by Symons et al (U.S. 2003/0105881). Reconsideration and withdrawal of these rejections is respectfully requested in light of the remarks contained below.

Fundamental Distinction between Cited Art and Claimed Embodiments

Applicant respectfully traverses the rejections of claims 1-16 of the present application for reasons that will be specifically addressed in following paragraphs. However, before addressing the details of specific rejections, Applicant notes that there are fundamental differences between the claimed embodiments and the cited Symons reference.

In this regard, the embodiments of the present application are generally directed to methods for detecting unauthorized hardware devices in a local area network, comprising scanning ports of a plurality of hardware devices to retrieve MAC addresses thereof, filtering an uplink port on each of the hardware devices to acquire a first MAC address list, calculating the number of MAC addresses of the filtered ports to acquire a second MAC address list, and subtracting the number of ports with more than two MAC addresses on the first MAC address list from the number of ports with more than two

MAC addresses on the second MAC address list, thereby obtaining at least one unauthorized MAC address.

As described in the specification, the embodiments detect multiple hardware devices, comprising network and computer devices, in a LAN and locates and excludes unauthenticated network and computer devices from the hardware devices, enabling network stability and security.

In contrast to the claimed embodiments, Symons discloses a method of managing a network, said method comprising: a) configuring a switch in said network to forward a packet received at a first port if an address associated with said packet is authorized for said first port; b) forwarding said packet if said address is authorized; and c) comparing a set of learned addresses against a set of expected addresses, said learned addresses comprising addresses associated with packets processed at a second port, said expected addresses derived from an expected configuration of said network.

The Office Action alleged that the technical features of the claimed embodiments are disclosed in the cited reference. However, Symons only relevantly discloses a similar network authentication process according to received packets. With respect to disclosure in Symons, a switch is programmed with MAC addresses, which are authorized for packets processed at each switch port, based on a device coupled to the switch port. A packet is forwarded via a switch port if the MAC address of the switch port is authorized. If not authorized, the packet is dropped. Furthermore, MAC addresses that are learned at a port connecting two switches in the fabric are compared to MAC addresses that are expected at that port, based on the physical topology of the

network. If an unexpected MAC address is detected, the topology may be traced to locate the host port through which the packet with the unauthorized MAC address entered the virtual network. Additionally, the physical topology of the network may be periodically compared to the expected topology to detect unexpected changes.

Relatively, the claimed embodiments assign at least two MAC addresses to every port of a network device, one for the port of the centralized communication cable device and the other for the computer hardware device, uses relevant communication protocol (such as SNMP) to identify unauthorized network devices or computer hardware devices, and issues warning messages to users and to administrators to terminate the detection procedure.

As described, Symons provides a method for detecting and preventing intrusion in a virtually-wired switching network, detecting and preventing such attacks which spring from inside the network, in which a packet can be forwarded via a port of a switch if the port is authorized. Relatively, the claimed embodiments detect network devices in a LAN to locate unauthorized devices according to the port number based on MAC addresses. Although port authorization is also performed in Symons, it implements different processing methods quite distinct from the claimed embodiments. Thus, the disclosure in Symons is clearly different than that of the claimed embodiments, and for at least this fundamental reason, the rejections should be withdrawn. In addition to these distinctions, each of the claim rejections will be independently addressed below.

Rejections of Claims 1 and 12

The Office Action rejected independent claims 1 and 12 as allegedly anticipated by Symons. Applicant respectfully disagrees.

Referring to claims 1 and 12, the claimed embodiments scan ports of a plurality of hardware devices to retrieve MAC addresses, filter an uplink port on each of the hardware devices to acquire a first MAC address list, calculate the number of MAC addresses of the filtered ports to acquire a second MAC address list, and perform a subtraction operation to obtains at least one unauthorized MAC address.

Specifically, claims 1 and 12 expressly recite:

> 1. A method for detecting unauthorized hardware devices in a local area network, comprising steps of:
>
> scanning ports of a plurality of hardware devices to retrieve MAC addresses thereof;
>
> filtering an uplink port on each of the hardware devices to acquire a first MAC address list;
>
> calculating the number of MAC addresses of the filtered ports to acquire a second MAC address list; and
>
> ***subtracting the number of ports with more than two MAC addresses on the first MAC address list from the number of ports with more than two MAC addresses on the second MAC address list, thereby obtaining at least one unauthorized MAC address.***
>
> 12. A storage medium containing a stored computer program providing a method for detecting unauthorized hardware devices, comprising using a computer to perform the steps of:
>
> scanning a plurality of ports of a plurality of hardware devices to retrieve MAC addresses thereof;
>
> filtering an uplink port of each hardware device to acquire a first MAC address list;
>
> calculating the number of MAC addresses of the ports of the network devices to acquire a second MAC address list; and
>
> ***subtracting the number of ports with more than two MAC addresses on the first MAC address list from the number of ports with more than two MAC addresses on the second MAC address list, thereby obtaining at least one unauthorized MAC address.***

(*Emphasis added*). Independent claims 1 and 12 patently define over Symons for at least the reason that Symons fails to disclose the feature emphasized above. In this regard, Symons does not disclose the subtraction step based on the first and second MAC address lists with the number of ports with more than two MAC addresses that obtains at least one unauthorized MAC address.

The Office Action cites paragraphs 0022, 0025-0026, 0048, 0058-0060, and 0066 as allegedly disclosing this feature. Applicant disagrees. In this regard, Application has reviewed each of these cited portions of Symons, and none teaches the claimed feature. In fact, an electronic search of the entire text of the Symons reference revealed that the word "subtract" does not even exist anywhere in the entire reference.

Thus, such a complete process and limitations are not disclosed in Symons, and the rejections of claims 1 and 12 should be withdrawn. As claims 2-6 and 13-16 depend from claims 1 and 12 respectively, the rejections of those claims should be withdrawn for at least the same reasons.

Rejection of Claims 2 and 13

In addition to the foregoing distinctions, Applicant submits that the rejections of claims 2 and 3 should be withdrawn for the following additional reasons. Referring to claims 2 and 13, the claimed embodiments compare the MAC addresses of the unauthorized hardware devices with MAC addresses in a routing entry table to obtain IP addresses of the unauthorized hardware devices, and acquire user information for the unauthorized hardware devices by SNMP or WINS services in accordance with the IP address of the unauthorized hardware devices. Symons, however, only relevantly

describes a packet can be forwarded if an address of a port is authorized, but not discloses acquires user information for the unauthorized hardware devices by SNMP or WINS services according to obtained IP addresses of the unauthorized hardware devices. For at least this additional reason, claims 2 and 13 define over Symons.

Rejection of Claims 3 and 14

Referring to claims 3 and 14, the embodiments define recursively scanning the ports of the authorized hardware devices by one of the authorized network devices. Symons discloses no such feature. For at least this additional reason, claims 3 and 14 define over Symons.

Rejection of Claim 7

Like claim 1, independent claim 7 has been rejected as allegedly anticipated by Symons. Applicant respectfully disagrees.

Referring to claim 7, the device detection unit scans a plurality of ports of a plurality of hardware devices to retrieve MAC addresses thereof, filters an uplink port of each hardware device to acquire a first MAC address list, and calculates the number of MAC addresses of the ports of the network devices to acquire a second MAC address list, and the device processing unit subtracts the number of ports with more than two MAC addresses on the first MAC address list from the number of ports with more than two MAC addresses on the second MAC address list, thereby obtaining at least one unauthorized MAC address.

Specifically, claim 7 recites:

7. A system for detecting unauthorized hardware devices in a local area network, comprising:

a device detection unit for scanning a plurality of ports of a plurality of hardware devices to retrieve MAC addresses thereof, filtering an uplink port of each hardware device to acquire a first MAC address list, and calculating the number of MAC addresses of the ports of the network devices to acquire a second MAC address list; and

a device processing unit, coupled with the device detection unit, for subtracting the number of ports with more than two MAC addresses on the first MAC address list from the number of ports with more than two MAC addresses on the second MAC address list, thereby obtaining at least one unauthorized MAC address.

(*Emphasis added.*) Claim 7 defines over Symons for at least the reason that Symons fails to disclose the feature emphasized above. As noted in connection with claim 1, Symons does not disclose the subtraction step based on the first and second MAC address lists with the number of ports with more than two MAC addresses that obtains at least one unauthorized MAC address. Therefore, Symons certainly doesn't disclose a processing unit that performs the subtracting.

For at least these reasons, claim 7 patently defines over Symons and the rejections should be withdrawn. As claims 8-11 depend from claim 7, the rejections of those claims should be withdrawn for at least the same reasons.

Rejection of Claim 8

In addition to the distinctions noted above, claim 8 defines a device processing unit that compares the MAC addresses of the unauthorized hardware devices with MAC addresses in a routing entry table to obtain IP addresses of unauthorized hardware devices, and acquire user information of the unauthorized hardware devices by SNMP or WINS services. Symons, however, only relevantly describes that a packet can be

forwarded if an address of a port is authorized, but not discloses acquires user information for the unauthorized hardware devices by SNMP or WINS services according to obtained IP addresses of the unauthorized hardware devices. For at least this additional reason, the rejection of claim 8 should be withdrawn.

Rejection of Claim 9

In addition to the distinctions noted above, claim 8 defines a device detection unit that recursively scans the ports of the authorized hardware devices by one of the authorized network devices. Symons, however, does not disclose such a feature. For at least this additional reason, the rejection of claim 9 should be withdrawn.

Conclusion

In view of the foregoing, it is believed that all pending claims are in proper condition for allowance. If the Examiner believes that a telephone conference would expedite the examination of the above-identified patent application, the Examiner is invited to call the undersigned.

No fee is believed to be due in connection with this amendment and response. If, however, any fee is deemed to be payable, you are hereby authorized to charge any such fee to Deposit Account No. 20-0778.

Respectfully submitted,

/Daniel R. McClure/

Daniel R. McClure
Registration No. 38,962

THOMAS, KAYDEN, HORSTEMEYER & RISLEY, L.L.P.
Suite 1750
100 Galleria Parkway N.W.
Atlanta, Georgia 30339
(770) 933-9500